VIA ELECTRONIC MAIL

April 10, 2008

Office of the Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue
Washington, DC 20580

Re: Comments on FTC Online Behavioral Advertising Principles

Dear Sirs and Madams:

HSBC Finance Corporation[1], and HSBC Bank USA, N.A., (collectively "HSBC"), welcome the opportunity to comment to the Federal Trade Commission ("FTC") on the proposals set forth in "Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles."

HSBC appreciates the FTC's efforts to educate consumers and protect them from the possible risks related to online behavioral marketing and browsing the Internet. In some cases, however, the proposed principles appear to address broad privacy issues, rather than the specific topic of online behavioral advertising activities. In addition, because the proposal does not clearly define the possible risks and concerns related to gathering online behavioral data, some of the proposed actions may not be warranted, particularly where they do not address actual risks or concerns.

Moreover, HSBC is concerned about unintended negative consequences of the proposed principles. Specific principles such as these may have a detrimental effect on the overall Internet economy. The information collected by many entities is essential in order for Internet services to work and have economic viability. The guidelines in the proposed principles conflict with existing privacy laws, rules, and regulations. Implementing the guidelines would therefore be complicated and expensive, and likely be infeasible.

Existing Guidance

There are numerous existing federal and state laws and regulations aimed at protecting an individual's privacy, and HSBC believes that these sufficiently protect customers who visit our websites. This existing framework of standards could be expanded to cover all Internet advertising.

[1] Among other companies, HSBC Finance Corporation wholly owns HSBC Auto Finance Inc., HSBC Consumer Lending (USA) Inc., Beneficial Company LLC, HSBC Mortgage Services Inc., HSBC Card Services Inc., HSBC Bank Nevada, N.A., and HFC Company LLC.

The Gramm-Leach-Bliley Act ("GLBA") is a major indication of congressional intent on protecting financial privacy. Financial institutions are governed by the GLBA's Section V provisions on privacy and security. Regulators have issued rules and extensive supervisory guidance on many aspects of privacy and security over the past eight years. The financial industry is well regulated in this area. Therefore, HSBC recommends that financial institutions be explicitly exempt from coverage by the proposed online principles. In the alternative, the principles should contain a provision to the effect that entities that are in compliance with GLBA are deemed to be in compliance with these guidelines.

The FTC issued guidelines regarding online advertising in the document entitled "Dot Com Disclosures: Information about Online Advertising." The FTC has consistently indicated that consumer protection laws that apply to commercial activities in other media also apply to the same activities when conducted online. The FTC Act's prohibition on "unfair or deceptive acts or practices" encompasses Internet advertising, marketing and sales. In addition, many FTC rules and guidelines are not limited to any particular medium used to disseminate claims or advertising, and therefore, apply to online activities. HSBC believes that the approach that federal financial regulators have adopted could be used as a model for promulgating security and privacy guidelines applicable to non-financial institutions. Issuing online principles consistent with the rules contained in GLBA would provide a model for consistent rules for data privacy regardless of medium or industry.

Other examples of existing guidelines and standards include those of the Direct Marketing Association, the Interactive Advertising Bureau, the Network Advertising Initiative, TRUSTe, the AICPA's Webtrust, and BBB*OnLine*.

Consumer Education

HSBC supports the objective of educating consumers about Internet practices and available technology. Consumers armed with such knowledge are aware that they may take appropriate actions to protect his or her personal information. The proposed online principles imply that the average consumer is unaware that one's Internet activity can be observed or tracked. Internet users need to presume that data about their identity and their Internet activity are being collected and used in numerous ways. Consumers must realize that Internet activity is not anonymous and that their activity is observed and collected by others, unless they take steps to limit such activities.

Average Internet users are generally more sophisticated than the proposed online principles assume. Internet users frequently make decisions about what to share, with the understanding that information and services are often only available after the users provide personal information. The more informed consumers are, the more likely it is that he or she will perceive reasonable and customary uses of personal data as benign, and will agree to provide more complete and truthful personal information in exchange for better functionality, improved service, less expense, and robust information access. The success of social networking sites is a prime example. Experienced users understand that they are exposing personal information and they make specific and careful choices about the websites they utilize in this manner.

Consumers also need to be aware of the available technology that can be used to take control of the information they do want to protect. Consumers have options to utilize browser controls, turn off cookies, delete cookies on a regular basis, block pop-ups, limit the types of sites visited, and limit the type of information shared on each site. More sophisticated users may want to utilize one of the anonymizer networks or products available. Perhaps online companies, along with consumer education providers, could be encouraged to give consumers information about the various technologies available. It is the

responsibility of each consumer to research the available technology and decide for themselves which options will work for their purposes.

Consumers are the ones in control of their online settings that turn the privacy switch on and off. Consumers can make choices about the Internet activity they participate in, as well as the technology that can be utilized to protect their privacy. Adequate privacy protection can be achieved by simple controls, detective cookies, and limiting one's disclosure of personal information. HSBC recommends allowing web site operators to address some of the FTC's concerns via informative sites and links. Placing information on the web site about how the customer benefits from the collection of information may be more helpful to the consumer than an opt-in system.

The FTC also should consider the large variety of computer types, machine configurations, corporate and personal firewall configurations, web browsers and browser configurations, and new technology as it becomes widely available. The FTC should issue guidance to consumers that reflects the variety and complexities of Internet usage.

Online Behavioral Marketing

The FTC's proposal includes a very broad definition of "behavioral marketing". In fact, "behavioral advertising" is not clearly defined in the FTC proposal. We recommend that the FTC limit its scope to tracking and use of information for marketing purposes. The principles should contain concise and consistent defined terms which will promote consistent usage throughout and allow for better consumer protection through clear communication. Concise definitions will also result in clear direction to industry and enhance compliance.

Proposed Principle 1 - Transparency and consumer control

Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.

Consumers need to be aware of data collection practices of each web site they visit to effectively protect their own privacy. Web sites should contain notices to provide information about an organization's data collection practices. HSBC has provided consumers with privacy notices for many years and could include additional information about online data collection practices.

HSBC is concerned that the proposed principle appears to require that consumers be given the right to "opt-in" to a particular web site owner's collection and use of their information. It also does not appear to limit this opt-in choice to any types of activities, such as requesting and using types of non-public personal information. This aspect of the principle needs to be clarified.

This principle exceeds the reasonable opt-out provisions of the GLBA as adopted by Congress. An opt-in approach would be difficult and costly for online companies and web site operators to implement. Businesses would be required to collect data and post cookies on visitors as they enter the site, in order to know whether they have opted-in. Because users often access web sites from various computers, the opt-

in would have to be entered each time. If the cookies get deleted, the consumer may have to opt-in multiple times. Both of these possibilities would cause confusion and frustration to the consumer.

Much of the online behavior tracking information collected by HSBC and other online companies occurs via "cookies". Through cookies, online companies can record what a particular consumer has an interest in, and how the consumer arrived at a particular web page. This is anonymous data that does not contain any non-public personal information, sensitive data, or page history. In order for online companies to implement an opt-in program that would apply at this early stage, they would have to collect a large amount of non-public personal information that is currently not collected because it is not needed. Ironically, the proposal would cause more transfers and disclosures of non-public personal information just to track information for an opt-in process, creating additional possibilities for data loss. Implementation of such a program would be very costly as well.

Effective Internet practices must balance the need for attractive web pages designed to achieve commercial goals, the need for consumers to be put on notice about data collection practices, and the reality that the majority of consumers do not read notices. On an individual level, consumers make a choice regarding the Internet services they want, the web sites they patronize, and the freedom to communicate and interact as they wish. In other words, consumers join the services they trust. If a service does not give them the assurances they want, and the matter is sufficiently important to them, they will find another provider. Requiring consumers to opt-in would likely limit the sites and services available to many consumers.

HSBC agrees that all information privacy disclosures should be clear and conspicuous, which would include notices about data collection on the Internet. Consumers could make an informed decision regarding whether to permit those data collection practices.

Proposed Principle 2 - Reasonable security, and limited data retention, for consumer data

Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.

Companies should retain data only as long as is necessary to fulfill a legitimate business or law enforcement need. FTC staff commends recent efforts by some industry members to reduce the time period for which they are retaining data. However, FTC staff seeks comment on whether companies can and should reduce their retention periods further.

With respect to security, we believe that companies involved in behavioral advertising should be required to provide reasonable security for the personally identifiable data they collect and maintain. We believe that the GLBA requirements provide the appropriate level of security required by financial institutions. Financial institutions have long been required to employ dynamic data protection safeguards to protect sensitive data. The FTC and federal financial regulators have already done excellent work in this area in developing the rules pursuant to the GLBA. Financial institutions have a strong track record in protecting customer information and in developing and deploying robust, risk-based, and dynamic information security programs that include authentication and encryption technologies. Because many organizations (not just financial institutions) store, transmit or process sensitive information, all organizations should be

required to guard personally identifiable information as stringently as entities covered by GLBA. HSBC recommends the adoption of consistent standards for all media and industries.

With respect to data retention time periods, financial institutions and companies under SEC oversight are subject to various regulatory document retention periods and otherwise retain discretion over document retention. Any guidance related to retention time periods should reflect these requirements, or provide for an exemption for those types of entities from coverage.

Proposed Principle 3 - Affirmative express consent for material changes to existing privacy policies

As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.

Online behavior patterns are important not just for advertising, but for other operational priorities such as fraud monitoring, compliance with regulatory or legal requirements, and website analytics. The FTC should also consider these other priorities in establishing principles. Requiring affirmative express consent for all of these types of activities would raise significant issues with respect to the service models that organizations have developed over many years. In addition, this is another inconsistency with the standards set forth in GLBA.

HSBC also recommends that the FTC consider the circumstances of mergers and acquisitions. For example, an acquiring company should be able to utilize its own notice practices (for example, by providing adequate prior notice) and continue to utilize information about the acquired company's customers without being required to obtain affirmative written opt-in, which would be difficult. Without this flexibility, the cost of mergers and acquisitions could rise. Alternatively, merger candidates may be less attractive. We believe this type of result is not intended by the FTC.

Proposed Principle 4 - Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising.

Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice.

Although HSBC generally agrees that an individual's information is not generally necessary for marketing purposes, it is important to provide a clear and targeted definition of "sensitive information" so that organizations are able to comply with this principle. We encourage the FTC not to define "sensitive information" overbroadly. In addition, entities should only have a duty to protect sensitive information of their customers, not consumers who briefly visit the web sites.

Proposed Principle 5 - Information on Tracking Data for Purposes Other Than Behavior Advertising

FTC staff seeks additional information about the potential uses of tracking data beyond behavioral advertising and, in particular: (1) which secondary uses raise concerns, (2) whether companies are in

fact using data for these secondary purposes, (3) whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data, and (4) whether secondary uses, if they occur, merit some form of heightened protection.

Financial institutions use data for numerous purposes including fraud detection, deterring security breaches, research and development, improved website design and content, and product development in order to meet the changing needs of customers. Efforts to limit the use of data could affect these important functions.

HSBC uses behavioral data for metrics and measures, security and fraud monitoring, and to ascertain customer insight in order to enhance product and service offerings. These functions generally rely only on non-personally identifiable data and do not require heightened protection. More specifically, HSBC and other organizations use the anonymous information to more effectively market the same type of products that have already been marketed to the same customers. Tracking data may be used for purposes of developing the right advertising message for the product (i.e. certain customers would receive one marketing message; others would receive a different marketing message). We believe this type of use is not the type of use the FTC intends to preclude in the proposed principles.

Conclusion

The requirements of GLBA provide the appropriate security and privacy protection for consumers and should be applied to non-financial institutions where appropriate. Uniform national standards for both information safeguards and notice should apply to all entities that maintain sensitive consumer information. Such standards should not be limited to commercial entities, but should also apply to other organizations (e.g., universities) that maintain significant amounts of sensitive non-public personal information. HSBC believes the focus should be on educating consumers.

Thank you for your consideration. If there are any questions concerning this letter, or if the FTC requires additional information, do not hesitate to contact Jeff Wood at 224-544-2948 or Patricia Grace at 716-841-5733.

Sincerely,

Jeffrey B. Wood, Esq.
HSBC Finance Corporation

Patricia Grace
Deputy General Counsel
HSBC Bank USA, National Association